REMARKS

Claims 115-121, 230-237, 286-287, 289, 292, 294, and 296 remain pending in the application. Claims 115-120, 230, 236-237, and 291 have been amended. No new matter was added by the aforementioned amendments.

Applicant has carefully reviewed the arguments presented in the Office Action and respectfully requests reconsideration of the application, as amended, in view of the remarks presented below.

Claim Rejections under 35 U.S.C. § 102(b)

Claims 115-121, 230-237, 286-287, 289, 292, 294, and 296 have been rejected under 35 U.S.C. § 102(b), as being anticipated by Barkan (International Publication No. WO 98/17042). Barkan teaches nine different methods in which a sender receives proof of an E-mail message delivered to a recipient. Nothing in Barkan, however, teaches or suggests maintaining the message and additionally creating a digital signature of the message for later authentication of the message by the server, and transmitting to the sender the message and the digital signature of the message before any authentication of the message for storage by the sender, as recited by amended Claim 115.

Methods 1 and 9 do not disclose a digital signature, or a hash or CRC, of the message for later authentication of the message by the server. In Methods 3-8, a hash or CRC is created by the E-mail program of the first user, not a server. (See, e.g., page 18, step (e), pages 22-23, steps (b)-(d), and pages 27-28, step (a)(3), pages 41-42, step (a)(3), and page 50, step (a)(4).)

Additionally, server is not disclosed in methods 1, 8 or 9. In method 2, authentication of the message is entirely achieved by a user email program and no authentication of any kind is done on a server. (See pages 18-21.) In method 3, an encrypted version of the message, the decryption key, and a hash are sent by the sender (first user) to either the receiving user (second user) or an intermediary server. (See page 22-23, steps (b)-(e).) The server or intermediary never sends the message to the sender. A receipt, not the message, and which may include a hash or CRC, is made available to the sender by the server only after the message identification is authenticated by the server. (Page 23-24, step (h).)

In method 4, the original message is encrypted by the sender using a symmetrical key, and the sender also creates a hash or CRC of the message. (See page 27-28, step (a).) The server never creates any digital signature of the message. Indeed, Balkan teaches that the Server 3 cannot read the message in section 41, since it is already encrypted. (Page 29, step (c)(1).) The server merely creates a new message by further encrypting the already encrypted message previously prepared and sent to the server by the sender. (See pages 29-30, step (c).) Because the message is not readable by the server, it is impossible for the server disclosed in Balkan to create a digital signature of the message. Moreover, the server sends an encrypted copy of the message (received from user 2) to the sender (user 1) only after the server compares an encrypted message previously sent to user 2 with the encrypted copy received from and further encrypted by user 2. (See page 32-33, step (h).) Specifically, only encrypted copies of the message passing through the server are compared. A hash or CRC or digital signature of the message is never used by the server. The message is only authenticated by the sender after receiving the encrypted version from the server. (See page 34, step (i)(4).) Thus, the message is not transmitted to the sender before any authentication of the message takes place, as recited by amended Claim 115.

Methods 5 teaches an automated version of method 4, and method 6 expands the previous methods by adding further encryption layers. Methods 5 and 6 do not teach or suggest Applicant's invention for the same reasons as method 4.

Lastly, method 7 teaches the server (referred to as Post Office) does not have access to the messages themselves. (See page 41.) User 1 sends an encrypted message directly to User 2, and a decryption key and hash or CRC to the server. (See page 42-44, steps (b)-(c).) If User 2 accepts the message then User 2 sends a receipt and the CRC to the server. (See page 45-46, step (f)(2).) The server merely compares the CRCs to determine if the correct message was received. (See page 46, step (h).) The server never creates a digital signature of the message. Furthermore, the server sends the receipt, not the message, to the sender only after the CRCs are compared.

Even if the nine methods of Barkan could be mixed and matched, nothing in Barkan teaches or suggests at the server creating a digital signature of the message for later authentication of the message by the server, and transmitting to the sender the message and the

digital signature of the message before any authentication of the message for storage by the sender, as recited by amended Claim 115. Particularly, no embodiment or method of Barkan teaches or teaches or suggests how the server is able to interpret, transcribe, or read the message such as to enable creating a digital signature from the message. Moreover, corresponding email systems of the sending and receiving users are relied on to create and process the hash or CRC, and the hash or CRC or digital signature is never created on the server. Indeed, Barkan teaches away from Claim 115 because "anyone can compute the CRC." (Page 28.) Unlike the system of Barkan which relies on the cooperation of special software at the recipient, Applicant's server is entirely responsible for creating a non-forgeable digital signature of the message, known only to the server, so that compliance of the recipient is not required. (See Disclosure as filed, page 3, lines 26-30, and page 11, line 29 to page 12, line 6.)

Barkan also does not teach or suggest transmitting the electronic attachment from the second server to the sender after the transmission of the message from the second server to the destination server but before any authentication of the message by the second server, as recited by Claim 230. The statement that an "intermediary participates in the transaction" does not teach or suggest authentication of any kind. (Abstract; page 12, step (c).) As already shown above, methods 1, 2, 8 and 9 do not use a server to authenticate a message of any kind. (See also page 12, steps (a)-(b).) In methods 3 and 7, a receipt is sent after authentication of the message. In Barkan, page 23-34, step (h), the server specifically refrains from sending a receipt until after a message identification is authenticated by the server. The server never authenticates the message itself. Furthermore, in methods 4, 5 and 6, nothing is transmitted to the sender before some type of comparison or authentication is performed by the server. Barkan, page 30, step (d), also cited by the examiner, teaches sending a message to user 2, not the sender (user 1). The server sends an encrypted copy of the message (received from user 2) to the sender (user 1) only after the server compares an encrypted message previously sent to user 2 with the encrypted copy received from and further encrypted by user 2. (See page 32-33, step (h); page 33, 1st paragraph.) Moreover, only encrypted copies of the message passing through the server are compared. The message itself is never authenticated by the server. The message is only authenticated by the sender after receiving the encrypted version from the server. (See page 34.) As can be seen, none of the methods of Barkan teach or suggest sending anything to the sender before any authentication of the message by the server.

As has been seen above, none of the methods in Barkan disclose all of the steps recited in Claim 115 or Claim 230 as required for a rejection under 35 U.S.C. § 102(b). Accordingly, Claim 115 and Claim 230, and the claims that depend therefrom, are patent ably distinguishable over the Barkan reference. Accordingly, reconsideration and allowance of the application are respectfully requested.

Claim Rejections under 35 U.S.C. § 103(a)

Claims 288, 290-291, 293, 295 and 297 have been rejected under 35 U.S.C. § 103(a), as being unpatentable over Barkan, International Publication No. WO 98/17042, in view of Zabetian, U.S. Patent No. 6,327,656.

Claims 288, 290-291, 293, 295 are dependent from Claim 115. For the reasons stated above, Barkan in view of Zabetian does not teach or suggest transmitting to the sender the message and the digital signature of the message before any authentication of the message for storage by the sender, as recited by amended Claim 115. Moreover, no embodiment or method of Barkan teaches or teaches or suggests how the server is able to interpret, transcribe, or read the message such as to enable creating a digital signature from the message. Corresponding email systems of the sending and receiving users are relied on to create and process the hash or CRC, and the hash or CRC or digital signature is never created on the server. Indeed, Barkan teaches away from Claim 115 because "anyone can compute the CRC." (Page 28.) Unlike the system of Barkan which relies on the cooperation of special software at the recipient, Applicant's server is entirely responsible for creating a non-forgeable digital signature of the message, known only to the server, so that compliance of the recipient is not required. (See Disclosure as filed, page 3, lines 26-30, and page 11, line 29 to page 12, line 6.)

For the same reasons Barkan does not teach or suggest transmitting the electronic attachment from the second server to the sender after the transmission of the message from the second server to the destination server but before any authentication of the message by the second server, as recited by Claim 230. Claim 297 is dependant from Claim 230. Therefore, it is improper to modify or substitute the email system of Barkan with the email system of Zabetian to achieve a server which sends the electronic attachment to the sender before authentication such as the present invention.

The portions of Barkan regarding when a message, receipt or other attachment is sent to the sender after the message is authenticated, or the openness of the CRC algorithm, that teach away from the claimed combination should not be ignored in a *prima facie* obviousness rejection. M.P.E.P. 2141.02 ¶ VI. ("a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention"). It is also noted that it is improper to use the present specification and claims to envision the claimed invention in hindsight. *Ex Parte Crawford et al.*, Appeal 20062429, Decided May 30, 2007. For the foregoing reasons, including the absence of claim elements in any of the cited references, withdrawal of the obviousness rejection and allowance of Claims 288, 290-291, 293, 295 and 297 is respectfully requested.

Should the Examiner have any questions concerning the above amendments and arguments, or any suggestions to obtain allowance, Applicant requests that the Examiner contact Applicant's attorney, John K. Fitzgerald, at 310-824-5555.

The Commissioner is authorized to credit any overpayment or charge any additional fees in this matter to our Deposit Account No. 06-2425.

Date: October 24, 2008

Respectfully submitted,

FULWIDER PATTON LLP

/john k. fitzgerald/
John K. Fitzgerald
Reg. No. 38,881

JKF:KCC:vmm:mlr

Howard Hughes Center
6060 Civic Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201
301243.1